

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-29844
(P2000-29844A)

(43)公開日 平成12年1月28日(2000.1.28)

| | | | |
|--------------------------|-------|---------------|-------------------|
| (51)Int.Cl. ⁷ | 識別記号 | F I | テーマコード(参考) |
| G 0 6 F 15/00 | 3 3 0 | G 0 6 F 15/00 | 3 3 0 C 5 B 0 8 5 |
| 13/00 | 3 5 5 | 13/00 | 3 5 5 5 B 0 8 9 |

審査請求 未請求 請求項の数9 O L (全 14 頁)

(21)出願番号 特願平10-192711

(22)出願日 平成10年7月8日(1998.7.8)

(71)出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72)発明者 土居 克良

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

(72)発明者 戸田 浩義

大阪府大阪市阿倍野区長池町22番22号 シ

ャープ株式会社内

(74)代理人 100064746

弁理士 深見 久郎

Fターム(参考) 5B085 AC01 AC12 AE04 AE06 BG07

5B089 AA21 AA22 AC03 CC17 DD03

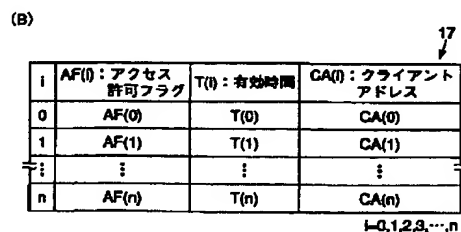
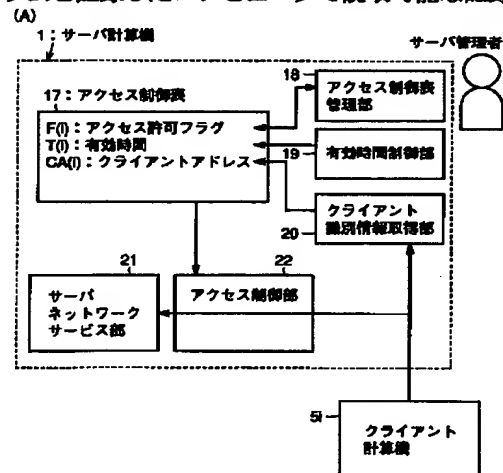
DD07

(54)【発明の名称】 通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置、ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒

(57)【要約】

【課題】 簡単かつ確実に特定クライアント計算機にのみサーバ計算機のアクセスが許可される通信ネットワークの簡易セキュリティ設定方法を提供する。

【解決手段】 サーバ計算機1はアクセス制御表17を参照しクライアント計算機5iのアクセス要求を許可する。表17には計算機5iについて、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されないとオフ設定されるアクセス許可フラグAF(i)と、所定期間内にアクセス要求とともに受信したクライアントアドレスCA(i)とが対応づけて登録される。フラグをオンして所定時間以内にアクセス要求が受信されれば、要求元計算機5iに対してのみ、以降のアクセス要求が許可される。



【特許請求の範囲】

【請求項 1】 1 台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定方法であって、

前記クライアント計算機のそれぞれにおいては、個々の識別情報とともに前記サーバ計算機にアクセス要求を送信する送信ステップを備え、

前記サーバ計算機においては、

前記クライアント計算機のうち同時に接続可能な所定台数分の前記クライアント計算機のそれぞれについて少なくとも、前記アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内に前記アクセス要求が受信されなければオフに設定されるフラグと、前記所定期間内に前記クライアント計算機から送信された前記アクセス要求とともに受信した前記識別情報とを対応づけて登録するためのテーブルを有して、

前記アクセス要求を受信したとき、前記アクセス要求とともに受信した前記識別情報と前記テーブルの識別情報とを照合する照合ステップと、

前記照合の結果において、前記テーブルの識別情報が空または両識別情報が一致し、かつ対応のフラグがオン状態である時は、受信された前記アクセス要求を許可するアクセス許可ステップとを備えた、通信ネットワークにおける簡易セキュリティ設定方法。

【請求項 2】 前記テーブルの内容は、外部からの入力内容に基づいて変更可能であることを特徴とする、請求項 1 に記載の通信ネットワークにおける簡易セキュリティ設定方法。

【請求項 3】 前記識別情報は、前記クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含み、前記照合結果における両識別情報が一致したときとは、前記両アドレス情報がそれぞれ一致したときであることを特徴とする、請求項 1 または 2 に記載の通信ネットワークにおける簡易セキュリティ設定方法。

【請求項 4】 1 台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定装置であって、

前記サーバ計算機において、

前記クライアント計算機のそれぞれから前記サーバ計算機へのアクセス要求を受信したとき、該受信内容から前記クライアント計算機の識別情報を取得する取得手段と、

前記クライアント計算機のうち同時に接続可能な所定台数分の前記クライアント計算機のそれぞれについて少なくとも、前記アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内に前記アクセス要求が受信されなければオフに設定されるフラグと、前記所定期間内に前記取得手段により

取得された前記識別情報とを対応づけて登録するためのテーブルと、前記アクセス要求を受信したとき、前記取得手段により取得された前記識別情報と前記テーブルの識別情報とを照合する照合手段と、

前記照合の結果において、前記テーブルの識別情報が空または両識別情報が一致して、かつ対応のフラグがオン状態である時は、受信した前記アクセス要求を許可するアクセス許可手段とを備えた、通信ネットワークにおける簡易セキュリティ設定装置。

10 【請求項 5】 前記テーブルの内容は、外部からの入力内容に基づいて変更可能であることを特徴とする、請求項 4 に記載の通信ネットワークにおける簡易セキュリティ設定装置。

【請求項 6】 前記識別情報は、前記クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含み、前記照合結果における両識別情報が一致したときとは、前記両アドレス情報がそれぞれ一致したときであることを特徴とする、請求項 4 または 5 に記載の通信ネットワークにおける簡易セキュリティ設定装置。

【請求項 7】 1 台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定方法をコンピュータに実行させるための簡易セキュリティ設定プログラムを記録したコンピュータ読取可能な記録媒体であって、前記簡易セキュリティ設定方法は、

前記クライアント計算機のそれぞれにおいて、個々の識別情報とともに前記サーバ計算機にアクセス要求を送信する送信ステップを備え、

30 前記サーバ計算機において、

前記クライアント計算機のうち同時に接続可能な所定台数分の前記クライアント計算機のそれぞれについて少なくとも、前記アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内に前記アクセス要求が受信されなければオフに設定されるフラグと、前記所定期間内に前記クライアント計算機から送信された前記アクセス要求とともに受信した前記識別情報とを対応づけて登録するためのテーブルを有し、

40 前記アクセス要求を受信したとき、前記アクセス要求とともに受信した前記識別情報と前記テーブルの識別情報とを照合する照合ステップと、

前記照合の結果において、前記テーブルの識別情報が空または両識別情報が一致して、かつ対応のフラグがオン状態である時は、受信された前記アクセス要求を許可するアクセス許可ステップとを備えた、通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体。

【請求項 8】 前記テーブルの内容は、外部からの入力内容に基づいて変更可能であることを特徴とする、請求

項 7 に記載の通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体。

【請求項 9】 前記識別情報は、前記クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含み、前記照合結果における両識別情報が一致したときとは、前記両アドレス情報がそれぞれ一致したときであることを特徴とする、請求項 7 または 8 に記載の通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明はサーバ計算機と 1 台以上のクライアント計算機が相互に通信接続されるような通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体であって、特に、サーバ計算機のサービス提供を特定のクライアント計算機にのみ許可する場合の通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体に関する。

【0002】

【従来の技術】 サーバ計算機がクライアント計算機とネットワークで結合され、クライアント計算機からの要求をサーバ計算機で処理するシステムは、クライアントサーバシステムと呼ばれ、以下のようなさまざまな方法でサービス提供に関するセキュリティの設定を行なっている。これにより、許可されるべき相手にのみサービス提供が許可されて、許可すべきでない相手にはサービス提供が行なわれないようにしている。

【0003】 第 1 の例として、たとえばサービス提供を許可すべきクライアント計算機の IP（インターネットプロトコルの略）アドレス範囲を事前にサーバ計算機に登録し、これに一致するクライアント計算機のみサービス提供を許可する方法がある。

【0004】 具体的には“World Wide Web（以下、WWWと略す）サーバ構築技法”インターフェイス 1995 年 9 月号 p p 151～167 においてサーバ計算機に予め記憶された IP アドレスまたはアドレス範囲に一致するアドレスを有するクライアント計算機からの要求のみを受付けてサービス提供を許可する方法がとられていた。

【0005】 たとえば、アドレス範囲パターンが 133.159.*.* であるとき、IP アドレスが 133.159.0.0 から 133.159.255.255 までのクライアント計算機にはサービスを許可する。それ以外のクライアント計算機に対してはサービス提供

の拒絶通知が行なわれる。

【0006】 第 2 例としては、たとえばクライアント計算機やサーバ計算機に通信接続する場合に、ユーザ名とパスワードを送信して、サーバ計算機は予め登録されたユーザ名とパスワードに一致する場合にのみアクセス要求を受付ける方式である。

【0007】 具体的には、WWWサーバにおける基本認証方式がこれに当たる。WWWサーバにおける基本認証方式ではクライアント計算機の WWW ブラウザがオンし WWWサーバ計算機の特定期間をアクセスしようとすると、ユーザ名とパスワードをクライアント計算機においてユーザに入力させ、予め WWWサーバ側に登録されていたものと一致したときのみ、WWWサーバの特定期間のアクセスを許可するものである。

【0008】 第 3 例としては、たとえば特開平 02-051397 号公報の回線受信端末装置に示されるものがある。回線受信端末装置として着信応答を許可する加入者番号を記憶しておき、この加入者番号と同じ番号の発信元からの着信だけを受付けることにより、被呼側では希望する発信元との間でだけ通信が行なえる方法が提案される。

【0009】 また第 4 例として特開平 02-036657 号公報の通信装置がある。この通信装置によれば着信を受付ける相手局の識別情報を記憶しておき、それ以外の相手局からの着信を拒否する方法が提供される。この着信拒否制御を無効化あるいは有効化する機能をもっているため、登録されていない相手局からの着信を面倒な操作なしに拒否可能にする方法が提供される。

【0010】 第 5 の例として、いわゆる迷惑電話防止システムにも類似の制御方法がある。一般に迷惑電話防止システムの採用する方式は、着信側はかかってきた迷惑電話の直後に電話を操作して電話局に対して所定信号を送信すれば、直前にかかってきた電話番号に対しては以後着信を拒否することができる。これは、電話局側の電話交換機が着信拒否識別番号を記憶するからである。

【0011】 このように通信ネットワークにおけるサーバ計算機に対するクライアント計算機のアクセス制御は、サーバ計算機側に着信許可識別情報を予め登録するか、着信拒否識別情報を予め登録する方法が一般的である。

【0012】

【発明が解決しようとする課題】 ところが、上述したようなアクセスを許可する（着信を許可する）クライアント計算機の識別番号（IP アドレスパターン）を予めサーバ計算機側に登録する方法では、クライアント計算機の IP アドレスが予め判明していなければならない、また、その識別情報である IP アドレス値をサーバ計算機に登録しておく必要がある。

【0013】 この場合、サーバクライアントシステムの利用者は、IP アドレスの概念を理解し数値で指定する

必要があり煩わしいという課題があった。これに関し、第5例では機械的に発信者識別番号を記憶させることで、以後着信許可／拒否が行なわれることで数値入力操作が不要となっている点で改善がみられる。

【0014】また、第2例のような基本認証方式では、クライアント計算機においてユーザ名とパスワードをユーザに入力させる煩雑な操作が必要であるという課題が残る。

【0015】また、第3および第4例の通信装置では、発呼側をクライアント計算機、着信側をサーバ計算機とすればサーバクライアントシステムのアクセス制御とみなせる。この場合、識別情報はアドレスに相当する。

【0016】また、上述の第4例では、予め着信応答する加入者番号を記憶しておくので第1例と同等である。

【0017】また、第5例では第1例同様アクセス許可されるクライアントのアドレスをサーバ側に登録しておく方式と同じであり、許可クライアント計算機のアドレスの事前登録が必要となっている。

【0018】第4例では着信許可する相手局の識別情報を予め登録する方式であるため、登録以外の局からかかってきた着信を拒否するので第1例に類似している。

【0019】第4例では着信拒否制御を無効にする手法を使って着信許可に切替える対応をとる必要がある。

【0020】それゆえにこの発明の目的は、簡単かつ確実に、特定のクライアント計算機に対してのみサーバ計算機へのアクセス要求が許可されるような通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体を提供することである。

【0021】

【課題を解決するための手段】請求項1に記載の通信ネットワークにおける簡易セキュリティ設定方法は、1台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおいて適用されて、以下のような特徴を有する。

【0022】クライアント計算機のそれぞれにおいては、個々の識別情報とともにサーバ計算機にアクセス要求を送信する送信ステップを備える。

【0023】サーバ計算機においては、クライアント計算機のうち同時に接続可能な所定台数分のクライアント計算機のそれぞれについて少なくとも、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されなければオフに設定されるフラグと、所定期間内にクライアント計算機から送信されたアクセス要求とともに受信した識別情報とを対応づけて登録するためのテーブルを有して、照合ステップと、アクセス許可ステップとを備える。

【0024】照合ステップはアクセス要求を受信したと

き、アクセス要求とともに受信した識別情報とテーブルの識別情報を照合する。

【0025】アクセス許可ステップは、照合ステップによる照合の結果において、テーブルの識別情報が空または両識別情報が一致し、かつ対応のフラグがオン状態である時は、受信したアクセス要求を許可する。

【0026】請求項1に記載の通信ネットワークにおける簡易セキュリティ設定方法によれば、サーバ計算機側でフラグがオンされてから所定期間内にサーバ計算機においてアクセス要求が受信されないと、フラグはオフされるから、所定期間内で最先にサーバ計算機に対してアクセス要求を送信したクライアント計算機に対してのみ、それ以降サーバ計算機側でそのアクセス要求が許可される。

【0027】したがって、サーバ計算機においてクライアント計算機の識別情報をアクセス許可パターンとして予め登録する必要がなく、サーバ計算機では簡単かつ確実に特定クライアント計算機からのアクセス要求のみ許可することができるような通信ネットワークにおけるアクセス許可に関するセキュリティを得ることができる。

【0028】また、一旦アクセス要求が許可されたクライアント計算機側では、サーバ計算機へのアクセス要求時にはパスワードなどの入力が必要となり、ユーザの使い勝手は向上する。

【0029】また、クライアント計算機とサーバ計算機のユーザが同一である場合、サーバ計算機側のテーブルでフラグがオンされたこと、すなわちサーバ計算機がアクセス要求を受理可能な状態に設定されたことを知り得るのは本人だけであるから、サーバ計算機には所定期間内に最先にアクセス要求したクライアント計算機のみ以降のアクセス要求が許可されるというこの方法では、アクセス要求時にユーザはアドレスの概念を知る必要はなく使い勝手が向上する。

【0030】また、あるユーザがフラグをオンして所定期間内にクライアント計算機を操作してアクセス要求を送信できない場合でも、所定期間内にアクセス要求がなければフラグはオフされるから、他のユーザによりクライアント計算機が操作されて不正にサーバ計算機側がアクセスされることが防止されて、該通信ネットワークにおけるアクセス許可に関するセキュリティは保障される。

【0031】請求項2に記載の通信ネットワークにおける簡易セキュリティ設定方法では、請求項1に記載の方法におけるテーブルの内容が、外部からの入力内容に基づいて変更可能である。

【0032】請求項2に記載の簡易セキュリティ設定方法によれば、サーバ計算機においてはテーブルの内容がたとえばユーザの所望する外部からの入力内容に基づいて変更され得る。

【0033】それゆえに、たとえば、テーブルの識別情

10

20

30

40

50

報またはフラグをユーザの所望するように変更できて、通信ネットワークにおいてサーバ計算機でアクセス要求が許可されるクライアント計算機を容易に設定または変更できる。言い換えれば、該通信ネットワークにおけるアクセス許可に関するセキュリティ内容がユーザの所望に応じて容易に設定および変更できる。

【0034】請求項3に記載の通信ネットワークにおける簡易セキュリティ設定方法は、請求項1または2に記載の簡易セキュリティ設定方法において、識別情報が、クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含む。そして、照合ステップによる照合結果における両識別情報が一致したときは、両アドレス情報がそれぞれ一致したときである。

【0035】請求項3に記載の通信ネットワークにおける簡易セキュリティ設定方法によれば、照合ステップにおいてアドレス情報の二重チェックが行なわれ、その結果によってクライアント計算機のサーバ計算機に対するアクセス要求が許可されるか否かが決定される。

【0036】それゆえに、アドレス情報の二重チェックにより不正なアクセス要求が許可されることは確実に回避されるから、簡単にセキュリティ内容の設定または変更が行なわれながらも、高いセキュリティレベルを得ることができる。

【0037】請求項4に記載の通信ネットワークにおける簡易セキュリティ設定装置は、1台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおいて適用されて、以下のような特徴を有する。

【0038】サーバ計算機においては、クライアント計算機のそれぞれからサーバ計算機へのアクセス要求を受信したとき、該受信内容からクライアント計算機の識別情報を取得する取得手段と、テーブルと、照合手段と、アクセス許可手段とを備える。

【0039】テーブルには、クライアント計算機のうち同時に接続可能な所定台数分のクライアント計算機のそれぞれについて少なくとも、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されなければオフに設定されるフラグと、所定期間内に取得手段により取得された識別情報とが対応づけて登録される。

【0040】照合手段は、アクセス要求を受信したとき、取得手段により取得された識別情報とテーブルの識別情報とを照合する。

【0041】アクセス許可手段は、上述の照合の結果において、テーブルの識別情報が空または両識別情報が一致して、かつ対応するフラグがオン状態である時は、受信したアクセス要求を許可する。

【0042】請求項4に記載の簡易セキュリティ設定装置によれば、フラグがオンされてから所定期間内にサーバ計算機においてアクセス要求が受信されないと、フラ

グはオフされるから、所定期間内で最先にサーバ計算機にアクセス要求を送信したクライアント計算機に対してのみそれ以降、そのアクセス要求がサーバ計算機側で許可される。

【0043】それゆえに、サーバ計算機において、クライアント計算機の識別情報をアクセス許可パターンとして予め登録する必要がなく、サーバ計算機では簡単かつ確実に特定クライアント計算機からのアクセス要求のみ許可することを保証するような通信ネットワークにおけるセキュリティを設定できる。

【0044】また、一旦アクセス要求が許可されたクライアント計算機においてもサーバ計算機へのアクセス要求時には、パスワードなどの入力が必要となつてユーザの使い勝手が向上する。

【0045】また、クライアント計算機とサーバ計算機のユーザが同一である場合、サーバ計算機側のテーブルでフラグがオンされたこと、すなわちサーバ計算機がアクセス要求を受理可能な状態に設定されたことを知り得るのは本人だけであるから、所定期間内に最先にアクセス要求したクライアント計算機のみ以降のアクセス要求が許可されるという上述の方法では、アクセス要求時にユーザはアドレスの概念を知る必要がなく使い勝手が向上する。

【0046】また、あるユーザがフラグをオンして所定期間内にクライアント計算機を操作してアクセス要求を送信できない場合でも、所定期間内にアクセス要求がなければフラグはオフされるので、他のユーザによりクライアント計算機が操作されて不正にサーバ計算機がアクセスされることが防止されて、該通信ネットワークにおけるアクセス許可に関するセキュリティは保障される。

【0047】請求項5に記載の通信ネットワークにおける簡易セキュリティ設定装置は、請求項4に記載の簡易セキュリティ設定装置におけるテーブルの内容が、外部からの入力内容に基づいて変更可能であるよう構成される。

【0048】請求項5に記載の簡易セキュリティ設定装置によれば、サーバ計算機においてはテーブルの内容がたとえばユーザの所望する外部からの入力内容に基づいて変更され得る。

【0049】それゆえに、たとえばテーブルの識別情報またはフラグをユーザの所望するように変更できて、該通信ネットワークにおけるアクセス許可に関するセキュリティ内容を容易に設定または変更できる。

【0050】請求項6に記載の通信ネットワークにおける簡易セキュリティ設定装置は、請求項4または5に記載の簡易セキュリティ設定装置における識別情報が、クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含む。

【0051】そして、上述の照合手段による照合結果に

おける両識別情報が一致したときとは、この両アドレス情報がそれぞれ一致したときであるよう構成される。

【0052】請求項6に記載の通信ネットワークにおける簡易セキュリティ設定装置によれば、照合手段のアドレス情報の二重チェックの結果に従ってアクセス許可手段がアクセス要求を許可するか否か決定するから、不正なアクセス要求を許可することが回避される。

【0053】これにより、簡単にセキュリティ内容の設定または変更が行なわれながらも、高いセキュリティレベルを得ることができる。

【0054】請求項7に記載の通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体は、簡易セキュリティ設定プログラムが、1台以上のクライアント計算機とサーバ計算機を相互に接続する通信ネットワークにおける簡易セキュリティ設定方法をコンピュータに実行させるためのものである。

【0055】この簡易セキュリティ設定方法は、クライアント計算機のそれぞれにおいて、個々の識別情報とともにサーバ計算機にアクセス要求を送信する送信ステップを備える。

【0056】サーバ計算機においては、照合ステップとアクセス許可ステップとを備える。照合ステップは、アクセス要求を受信したとき、クライアント計算機のうち同時に接続可能な所定台数分のクライアント計算機のそれぞれについて少なくとも、アクセス要求を許可するか否かに従いオンまたはオフに設定されるとともに、オン設定後、所定期間内にアクセス要求が受信されなければオフに設定されるフラグと、所定期間内にクライアント計算機から送信されたアクセス要求とともに受信した識別情報と対応づけて登録するためのテーブルを参照して、アクセス要求とともに受信した識別情報とこのテーブルの識別情報を照合する。

【0057】アクセス許可ステップは、照合ステップによる照合の結果において、テーブルの識別情報が空または両識別情報が一致して、かつ対応のフラグがオン状態である時は受信したアクセス要求を許可する。

【0058】請求項7によれば、サーバ計算機でフラグがオンされてから所定期間内にサーバ計算機においてアクセス要求が受信されないと、フラグはオフされるから、所定期間内で最先にサーバ計算機に対してアクセス要求を送信したクライアント計算機に対してのみそれ以降、そのアクセス要求がサーバ計算機側で許可される。

【0059】したがって、サーバ計算機においてクライアント計算機の識別情報をアクセス許可パターンとして予め登録する必要はなく、サーバ計算機においては簡単かつ確実に特定クライアント計算機からのアクセス要求のみ許可することを保証するような通信ネットワークにおけるセキュリティを構築できる。

【0060】また、一旦アクセス要求が許可されたクラ

イアント計算機側においても、サーバ計算機のアクセス要求時にはパスワードなどの入力不要となって、ユーザの使い勝手は向上する。

【0061】また、クライアント計算機とサーバ計算機のユーザが同一である場合、サーバ計算機側のテーブルでフラグがオンされたことを、すなわちサーバ計算機がアクセス要求を受理可能な状態に設定されたことを知り得るのは本人だけであるから、所定期間内に最先にアクセス要求したクライアント計算機のみ以降のアクセス要求が許可されるというこの方法では、アクセス要求時にユーザはアドレスの概念を知る必要がなく使い勝手が向上する。

【0062】また、あるユーザがフラグをオンして所定期間内にクライアント計算機を操作しアクセス要求を送信できない場合でも、所定期間内にアクセス要求がなければフラグがオフされるので、他のユーザによりクライアント計算機が操作され不正にサーバ計算機がアクセスされることが防止されて、該通信ネットワークにおけるアクセス許可に関するセキュリティが保障される。

【0063】請求項8に記載の通信ネットワークにおける簡易セキュリティ設定方法は、請求項7に記載の方法のテーブルの内容が、外部からの入力内容に基づいて変更可能であるよう構成される。

【0064】これにより、サーバ計算機においてはテーブルの内容がたとえばユーザの所望する外部からの入力内容に基づいて変更され得る。

【0065】それゆえに、たとえばテーブル上の識別情報またはフラグをユーザの所望するように変更できて、該通信ネットワークにおけるアクセス許可に関するセキュリティ内容をユーザの所望に応じて容易に設定または変更できる。

【0066】請求項9に記載の通信ネットワークにおける簡易セキュリティ設定方法は、請求項7または8に記載の方法における識別情報は、クライアント計算機を一意に識別するための任意に変更可能なアドレス情報および変更不可能なアドレス情報を含んで、照合ステップによる照合結果で両識別情報が一致したときとは、この両アドレス情報がそれぞれ一致したときであるよう構成される。

【0067】これにより、照合ステップによりアドレス情報の二重チェックが行なわれて、アクセス許可ステップはその結果に従ってアクセス要求を許可するか否か決定するので、不正なアクセス要求を許可することが回避される。

【0068】これにより、簡単にアクセス許可に関するセキュリティ内容の設定または変更が行なわれながらも、高いセキュリティレベルを得ることができる。

【0069】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照し詳細に説明する。

【0070】図1(A)と(B)は、この発明の実施の形態によるサーバ計算機1の機能構成とアクセス制御表とを示す図である。

【0071】図2は、この発明の実施の形態による通信ネットワークの構成図である。図2において、通信ネットワークは通信回線、たとえばイーサネットと、サーバ計算機1とイーサネットを介してサーバ計算機1から各種のサービスが提供され得る複数のクライアント計算機5*i* (*i*=0、1、2、3、…、*n*)を含む。

【0072】図示されるように、クライアント計算機5*i*はアクセス要求の発呼側であり、サーバ計算機1はアクセス要求の着呼側である。

【0073】図3は、図2のサーバ計算機1のブロック構成図である。図3においてサーバ計算機1は、計算機1自体を集中的に制御および管理するためのCPU11、各種データおよびプログラムを格納するためのメモリ12、たとえばハードディスクまたはフラッシュメモリなどからなり各種ソフトウェアおよび後述するアクセス制御表17を格納するための不揮発メモリ13、たとえばキーボードおよびマウスなどからなり外部操作されてデータを入力するための入力部14、たとえばCRTまたは液晶などからなる表示部15、イーサネットと該サーバ計算機1とのインターフェイスであるネットワークI/O16およびこれら各部を接続するバス10を含む。

【0074】サーバ計算機1におけるネットワークI/O16を介したクライアント計算機5*i*へのサービス提供は、不揮発メモリ13からサーバ用のソフトウェアがメモリ12に読込まれて、CPU11の制御の下に実行制御されることにより実現される。

【0075】図1(A)にはサーバ計算機1の機能構成が示され、図1(B)には図1(A)に示されるアクセス制御表17の構成例が示される。

【0076】図1(A)においてサーバ計算機1は接続される各クライアント計算機5*i*に関する該サーバ計算機1に対するアクセス要求を制御するための情報が格納されるアクセス制御表17、アクセス制御表17に関連のアクセス制御表管理部18、有効時間制御部19、クライアント識別情報取得部20およびアクセス制御部22、ならびにサーバネットワークサービス部21を含む。

【0077】アクセス制御表17は図1(B)に示されるようにクライアント計算機5*i*のうちサーバ計算機1に同時に接続してサービス提供を受けることができる所定台数分のクライアント計算機5*i*のそれぞれに対応して識別情報であるクライアントアドレスCA(*i*)、該サーバ計算機1へのアクセス要求の許可/不許可を示すアクセス許可フラグAF(*i*)および有効時間T(*i*)をデータ配列にして含む。

【0078】アクセス許可フラグAF(*i*)はアクセス

要求の許可/不許可をオンまたはオフのブール型変数で示し、有効時間T(*i*)は秒単位の変数である。クライアントアドレスCA(*i*)は整数型の変数であり、ここでは説明を簡単にするためにIPアドレス(TCP/IP)の4オクテッドアドレスを使用するが、イーサネットのMAC(media access control)アドレスであってもよい。

【0079】アクセス許可フラグAF(*i*)の初期値はオフであり、有効時間T(*i*)の初期値は0であり、クライアントアドレスA(*i*)の初期値は空である。

【0080】アクセス許可フラグAF(*i*)は、サーバ計算機1の管理者が入力部14を操作することによりオン(許可)オフ(不許可)設定される。

【0081】アクセス許可フラグAF(*i*)はオフからオンに設定されると、その後一定時間オン状態が維持される。

【0082】有効時間T(*i*)は対応のアクセス許可フラグAF(*i*)がオン状態に維持されているべき残り時間を示す。

【0083】アクセス制御表管理部18はサーバ計算機1の管理者がアクセス制御表17を表示部15に表示しながら入力部14を操作してアクセス制御表17の内容を更新(データの書込、消去および変更)するのを制御する。

【0084】有効時間制御部19は有効時間T(*i*)を設定および更新しながら対応のアクセス許可フラグAF(*i*)をオフに設定する。

【0085】詳細には、アクセス許可フラグAF(*i*)がサーバ管理者によりオフからオン設定されると、対応の有効時間T(*i*)に前述の一定期間を示す値を設定して、その後計時しながら有効時間T(*i*)を減算して更新する。有効時間制御部19は減算により有効時間T(*i*)が0になると、対応するアクセス許可フラグAF(*i*)をオンからオフにセットする。

【0086】クライアント識別情報取得部20は、サーバ計算機1に対してアクセス要求したクライアント計算機5*i*のアクセス要求とともに受理する識別情報を取得して、クライアントアドレスCA(*i*)としてアクセス制御表17に設定する。

【0087】アクセス制御部22はサーバ計算機1にアクセス要求したクライアント計算機5*i*について、アクセス制御表17の内容に基づいてサーバ計算機1に対するアクセス許可または不許可を制御する。

【0088】サーバネットワークサービス部21はアクセス要求したクライアント計算機5*i*が要求するサービス内容を認識して、要求されたサービスをクライアント計算機5*i*に提供する。

【0089】図4は、この発明の実施の形態によるサーバ計算機1におけるクライアント計算機5*i*からのアクセス要求の許可/不許可を制御するための手順を示すフ

10

20

30

40

50

ローチャートである。

【0090】図5は、図4のフローチャートに従う処理に並行して実行される有効時間T(i)の減算処理のフローチャートである。

【0091】図4と図5のフローチャートは予めプログラムにしてメモリ12にストアされCPU11の制御の下に実行される。

【0092】図6は、この発明の実施の形態によるサーバ計算機1において一定の有効時間T(i)内にクライアント計算機5iのアドレス学習が行なわれた場合の動作を示すタイミングチャートである。

【0093】図7は、この発明の実施の形態によるサーバ計算機1において、一定の有効時間T(i)内にクライアント計算機5iのアドレス学習が行なわれなかった場合の動作を示すタイミングチャートである。

【0094】なお、アドレス学習とは、クライアント計算機5iのIPアドレスなどの識別情報がクライアントアドレスCA(i)としてアクセス制御表17に登録される動作をいう。

【0095】図8～図13は、この発明の実施の形態によるクライアント計算機5iとサーバ計算機1間の通信に伴って更新されるアクセス制御表17の内容の第1～第6例を示す図である。

【0096】図14は、この発明の実施の形態によるアクセス制御表17の書換を説明する図である。

【0097】サーバ管理者は、アクセス制御表17の内容を設定または変更するために書換えようとする場合、入力部14を操作する。この操作に応じてアクセス制御表管理部18は不揮発メモリ13からアクセス制御表17を讀出して表示部15に図14のように表示する。

【0098】この表示内容を見て、サーバ管理者は入力部14を操作し、アクセス制御表17の内容を所望するように設定または変更することができる。

【0099】図14では、矢印のマウスカースルで、許可フラグAF(i)を示す許可チェックBOX(左端)にチェック印を入れると、対応するクライアントアドレス(123.45.67.89)のアドレス学習が可能となる。また、アドレスリセット(右端)をチェックすると対応するクライアントアドレスCA(i)に関するアドレス学習の内容が消去される。なお、アクセス制御表17のクライアントアドレスCA(i)の内容は、マウスカースルとキーボードを併用して修正変更することも可能である。

【0100】次に、図4と図5を参照しながら、図1のサーバ計算機1におけるクライアント計算機5iのアクセス要求の制御に関して説明する。

【0101】まず、サーバ計算機1が電源投入されて初期状態にあるとき、アクセス制御表管理部18はアクセス制御表17に初期値を設定する。

【0102】なお、ここでアクセス制御表17のデータ

配列の大きさを示す変数MAXの値を3と想定する。すなわちサーバ計算機1が同時に通信接続してサービス提供が可能なクライアント計算機5iは最大3台であると想定する。

【0103】クライアント計算機5iがサーバ計算機1にアクセスする。ここではサーバ計算機1のTCP/IPの8080番で動作しているサーバに対してコネクションを受けたとする。サーバ計算機1ではメモリ12上に展開されたサーバネットワークサービス部21がCPU11に制御され、ネットワーク制御を行なってサービスの受入れを待機する。サーバネットワークサービス部21のソフトウェアとしてWWWサーバが想定される。

【0104】まず、サーバ管理者は1台のクライアント計算機5iにのみサーバ計算機1に対するアクセス要求の許可を与えるために、アクセス制御表管理部18を介してアクセス許可フラグAF(0)のみオンに設定したと想定する。

【0105】このとき、アクセス許可フラグAF(0)がオフからオンに設定されるので、有効時間制御部19は対応の有効時間T(0)に一定時間期間としてたとえば30秒を設定して図5のフローチャートに従う以下の処理を実行する。

【0106】図5のフローチャートはCPU11の制御により1秒ごとに起動される有効時間制御部19による割込処理である。

【0107】有効時間制御部19は、図5の割込処理が起動されると配列データである有効時間T(i)の配列要素ポインタiを1ずつインクリメントしながら、ポインタiが配列の大きさMAX(=3)となるまで、アクセス制御表17中の有効時間T(i)のうちその値が>0であるものについて、値を1減算する(S20～S25)。

【0108】減算結果、有効時間T(i)が0になり、かつ対応のクライアントアドレスCA(i)の内容が“空”であれば、対応するアクセス許可フラグAF(i)をオフに設定する。

【0109】その後、該割込処理は終了する。以上のようにより、サーバ管理者によりアクセス許可フラグAF(i)がオンに設定された後に、対応の有効時間T(i)に設定された一定時間期間(30秒)内に対応のクライアントアドレスCA(i)についてアドレス学習が行なわれなければ、アクセス許可フラグAF(i)は有効時間制御部19により強制的にオンからオフに変更されて、サーバ計算機1へのクライアント計算機5iによるアクセス要求が一切許可されなくなる。

【0110】したがって、サーバ管理者が所望するクライアント計算機5iにのみアクセス要求を許可するためにアクセス許可フラグAF(i)をオンに設定し、その後有効時間T(i)の一定時間期間内にクライアント計算機5iから送信されたアクセス要求がサーバ計算機1

10

20

30

40

50

で受信されて許可されれば、その後は該クライアント計算機 5 i についてはサーバ計算機 1 へのアクセス要求が許可されるようにアクセス制御表 17 が設定される。

【0111】図 4 を参照して、サーバネットワークサービス部 21 はサーバ計算機 1 の 8080 番のポート番号でサーバソケットをオープンし、コネクションを受け付ける態勢に入る (S1)。

【0112】次に、クライアント計算機 5 i からサーバ計算機 1 に対してアクセス要求が送信されると、クライアント識別情報取得部 20 はネットワーク I/O 16 を介して受理したパケット中のクライアント計算機 5 i の IP アドレスを取得して、これを変数 CADDR に設定する。この操作は TCP/IP の基本であるので詳細は省略する (S2)。

【0113】次に、アクセス制御表管理部 18 はポインタ i を 0 から MAX まで 1 つずつインクリメントしながら次の処理を行なう。

【0114】アクセス制御表 17 のクライアントアドレス CA (i) を検索し、クライアントアドレス CA

(i) と変数 CADDR の内容が一致するものがあるか比較する (S4)。

【0115】一致するならば次の S5 の処理へ、一致しないならばポインタ i を +1 インクリメントして次のクライアントアドレス CA (i) について同様に処理をする (S41)。

【0116】アクセス許可フラグ AF (i) がオンならば (S5 で YES)、アクセス要求元のクライアント計算機 5 i にアクセス要求を許可してサービス提供を許可する (S6)。その後、S1 の処理に移行する。アクセス許可フラグ AF (i) がオンでないならば (S5 で NO)、アクセス要求したクライアント計算機 5 i に対してアクセス要求を許可しない旨の通知をしてサーバ計算機 1 によるサービスの提供を拒否する (S7)。その後、S1 の処理に移行する。

【0117】アクセス要求したクライアント計算機 5 i から取得した IP アドレスに一致するクライアントアドレス CA (i) がなければ (S42 で YES)、ポインタを 1 から MAX まで 1 つずつインクリメントしながら次の処理を行なう。まず、クライアントアドレス CA

(i) の内容が空であれば (S8 で YES)、該クライアントアドレス CA (i) に変数 CADDR の内容、すなわちアクセス要求したクライアント計算機 5 i から取得した IP アドレスを設定してアドレス学習し (S9)、対応の許可フラグ AF (i) がオンなら (S10 で YES)、アクセス要求したクライアント計算機 5 i にアクセス要求を許可してサービス提供を開始する (S11)。一方、オフならば (S10 で NO)、アクセス要求したクライアント計算機 5 i にアクセス要求の不許可を通知してサービス提供を拒否する (S12)。その後は、再度次のアクセス要求を待つ状態 (S1) に戻る。

【0118】一方、アクセス制御表 17 に空であるクライアントアドレス CA (i) がなければ (S82 で YES)、アクセス要求したクライアント計算機 5 i に対してアクセス要求の不許可を通知してサービス提供を拒否し (S12)、次のアクセス要求を待つ状態 (S1) に戻る。

【0119】図 4 のフローチャートに従う動作をより具体的に説明する。今、3 台のクライアント計算機 5 i としてクライアント計算機 50、51 および 52 がネットワーク上にあって、それぞれ 123、45、67、89、123、45、67、90、および 123、145、67、91 で示されるアドレスを識別情報として有していたとする。

【0120】まず、始めに図 8 のアクセス制御表 17 のようにサーバ管理者により 1 つのアクセス許可フラグ AF (0) だけオン設定され、対応の有効時間 T (0) に 30 秒が設定されて、1 台のクライアント計算機にのみアクセス要求の許可を与えるように設定したと想定する。

【0121】このとき、クライアント計算機 50 が有効時間 T (1) の 30 秒以内にサーバ計算機 1 にアクセス要求したとすると、アクセス制御表 17 の内容は図 9 のように更新されて、クライアント計算機 50 はサーバ計算機 1 に対するアクセスが許可されて、サービス提供が開始される。

【0122】この場合の有効時間 T (0) の経過に伴う許可フラグ AF (0) とクライアントアドレス CA

(0) の内容の変化が図 6 のタイミングチャートに示される。

【0123】続いて、クライアント計算機 51 がサーバ計算機 1 にアクセス要求を送信するとアクセス制御表 17 は図 10 のように更新される。

【0124】したがって、クライアント計算機 51 はサーバ計算機 1 においてアクセス要求が不許可となってサービス提供を受けることができない。

【0125】次に、図 1 (A) のアクセス制御表管理部 18 と有効時間制御部 19 の動作を述べる。サーバ管理者は表示部 15 に表示されたアクセス制御表 17 のアクセス許可フラグ AF (1) を入力部 14 を操作してオンに変更した後に、再度、クライアント計算機 51 からアクセス要求が送信された場合のアクセス制御表 17 の内容が図 11 に示される。

【0126】次にサーバ管理者が同様に図 12 のようにアクセス制御表 17 の 3 番目に登録されるアクセス許可フラグ AF (2) をオンに設定変更したとする。このとき、対応のクライアントアドレス CA (2) は空であるので、対応の有効時間 T (2) には 30 秒がセットされる。

【0127】ここで、アクセス許可フラグ AF (2) がオン設定されてから、50 秒経過後にクライアント計算

機 5 2 がサーバ計算機 1 にアクセス要求を送信する。この場合、アクセス制御表 1 7 の有効時間 T (2) は図 1 3 のように 0 となって、対応の許可フラグ A F (2) は有効時間制御部 1 9 によって既にオフとされているため、このアクセス要求は不許可となる。

【0128】この場合の、有効時間 T (2) の経過に伴うアクセス許可フラグ A F (2) とクライアントアドレス C A (2) の変化が図 7 のタイミングチャートに示される。

【0129】図 1 3 では、クライアント計算機 5 2 のアドレスがクライアントアドレス C A (2) としてアドレス学習されるから、後で、サーバ管理者がアクセス制御表管理部 1 8 を介して対応のアクセス許可フラグ A F (2) をオンに設定することで、クライアント計算機 5 2 に対して以降アクセス要求が許可されるように設定することができる。

【0130】なお、本実施の形態では、クライアントアドレス C A (i) として T C P / I P の I P アドレスを用いたが、I P アドレスをイーサネットインターフェイスの固有の M A C (Media Access Control) アドレスに変換してから用いるようにしてもよい。

【0131】クライアント計算機 5 i の電源投入ごとに I P アドレスの異なる可能性のある方式として D H C P によるアドレスの動的割当の場合がある (R. Droms RFC 1531 Dynamic Host Configuration Protocol 参照) からである。

【0132】このようにアクセス制御表 1 7 を用いた方法では、既にサーバ計算機 1 からアクセス要求が許可されてサービス提供を受けているクライアント計算機 5 i に優先的に排他的にサーバ計算機 1 のサービスの利用権が与えられ、かつ許可フラグ A F (i) をオンにしてから一定時間以内にアクセス要求したクライアント計算機 5 i 以外はアクセス要求が許可されない。

【0133】このようなシステムの利用方法としては、サーバ計算機 1 とクライアント計算機 5 i の利用者が同一人物であり、サーバ計算機 1 側で、許可フラグ A F (i) をオンに設定し、一定時間期間内にクライアント計算機 5 i からサーバ計算機 1 にアクセス要求を送信することによりクライアント計算機 5 i の識別情報をアクセス制御表 1 7 にアドレス学習させて、以後、他のクライアント計算機 5 i のサーバ計算機 1 の利用が拒否されるようにできる。

【0134】なお、有効時間 T (i) の示す一定時間期間内にこのアドレス学習が完了できない場合は作業が中断したとみなして、再度、許可フラグ A F (i) をオンにしなければならない。これにより、作業中断が発生しても、自動的に安全側に移行して、他の任意のクライアント計算機 5 i からサーバ計算機 1 が不正にアクセスされることが防止される。

【0135】上述した動作においては、予め定められた

数のクライアント計算機 5 i に対して、最初にアクセス要求を送信しアクセス制御表 1 7 のクライアントアドレス C A (i) の空欄を埋めることができたクライアント計算機 5 i のみ、それ以後サーバ計算機 1 の利用が可能になっていることがわかる。

【0136】このように、サーバ管理者は、クライアント計算機 5 i のアドレスをサービス許可パターンとしてサーバ計算機 1 に予め登録する必要がなく、簡単に特定のクライアント計算機 5 i からのアクセス要求のみを許可してサービス提供をするよう限定できる。

【0137】また、クライアント計算機 5 i とサーバ計算機 1 の管理者が同一人物であれば、サーバ計算機 1 でのサービス開始直後 (アクセス許可フラグ A F (i) がオンに設定された後) にクライアント計算機 5 i 側でサーバ計算機 1 がサービス提供可能であることを知る得るのは本人だけであり、サービス開始直後にサーバ計算機 1 に最初にアクセス要求を送信したクライアント計算機 5 i のみ、以後のサービス提供を受けることが可能になるという本方式では、アクセス制御においてユーザはアドレスの概念を知る必要がなくなって、使い勝手が向上する。

【0138】また、ユーザはクライアント計算機 5 i を用いてサーバ計算機 1 を利用するときにパスワードなどの入力が必要になり、使い勝手が向上する。また、クライアント計算機 5 i のアドレスはサーバ計算機 1 の不揮発メモリ 1 3 に記憶されるので、サーバ計算機 1 が電源を切って、また再起動した場合でもアクセス制御表 1 7 にアドレス学習された特定クライアント計算機 5 i のみに継続的にサービス提供することが可能となる。

【0139】また、図 1 4 に示されたように入力部 1 4 を介してアクセス制御表 1 7 の内容を書換えることによって新たなクライアント計算機 5 i のアクセス要求を許可するように設定できる。たとえば、許可フラグ A F (i) をオンに設定し、対応のクライアントアドレス C A (i) を空にしておくだけで、新たなクライアント計算機 5 i にサーバ計算機 1 のアクセス許可を与えることができる。

【0140】なお、上述した本実施の形態では、アクセス制御表 1 7 に学習された I P アドレスとアクセス要求とともに受信した I P アドレスとを照合しているが、これに限定されない。例えば、クライアント計算機側で任意に変更可能な I P アドレスとクライアント計算機側に固定に設定されて変更不可能な M A C アドレスとを用いて照合するようにしてもよい。

【0141】つまり、アクセス制御表 1 7 の I P アドレスとアクセス要求とともに受信した I P アドレス同士を照合して一致しても、アクセス制御表 1 7 の M A C アドレスとアクセス要求とともに受信した M A C アドレス同士の照合結果が不一致であれば、アクセス要求元のクライアント計算機 5 i にアクセス要求を許可せずに、その

旨をユーザに通知するようにしてもよい。これによりアドレスの2重チェックが行なわれ、不正アクセスを確実に回避できる。この場合、図14の画面ではMACアドレスの表示は省略される。

【0142】また、サーバ計算機1が個人が携帯するコンピュータであり、クライアント計算機5iがネットワークに固定して接続されたコンピュータである場合には、他の任意のクライアント計算機5iからサーバ計算機1が不用意にアクセスされて、サーバ計算機1の個人の情報が無断でアクセスされることが簡単かつ効果的に防止される。

【0143】今回か開示された実施の形態は全ての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 (A)と(B)は、この発明の実施の形態によるサーバ計算機の機能構成とアクセス制御表とを示す図である。

【図2】 この発明の実施の形態による通信ネットワークの構成図である。

【図3】 図2のサーバ計算機のブロック構成図である。

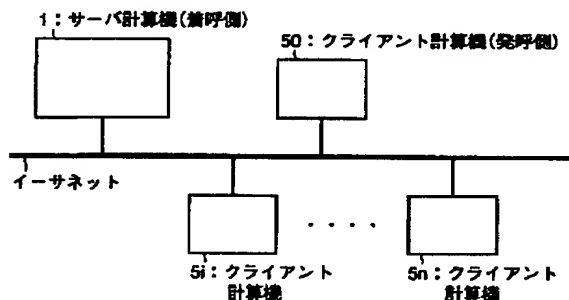
【図4】 この発明の実施の形態によるサーバ計算機におけるクライアント計算機からのアクセス要求の許可/不許可を制御するための手順を示すフローチャートである。

【図5】 図4のフローチャートに従う処理に並行して実行される有効時間の減算処理のフローチャートである。

【図6】 この発明の実施の形態によるサーバ計算機において、一定の有効時間内にクライアント計算機のアドレス学習が行なわれた場合の動作を示すタイミングチャートである。

【図7】 この発明の実施の形態によるサーバ計算機において、一定の有効時間内にクライアント計算機のアドレス学習が行なわれなかった場合の動作を示すタイミング

【図2】



チャートである。

【図8】 この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第1例を示す図である。

【図9】 この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第2例を示す図である。

【図10】 この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第3例を示す図である。

【図11】 この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第4例を示す図である。

【図12】 この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第5例を示す図である。

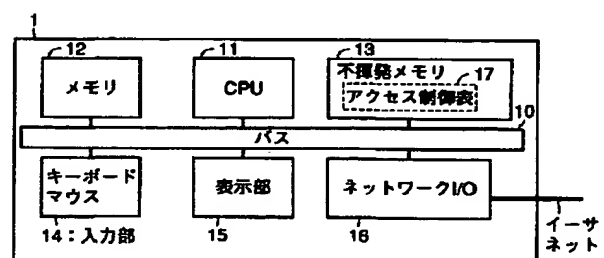
【図13】 この発明の実施の形態によるクライアント計算機とサーバ計算機間の通信に伴って更新されるアクセス制御表の内容の第6例を示す図である。

【図14】 この発明の実施の形態によるアクセス制御表の書換を説明する図である。

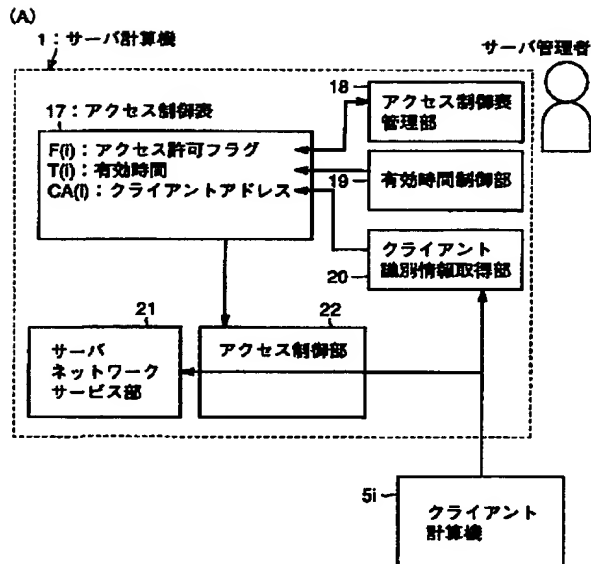
【符号の説明】

- 1 サーバ計算機
 - 5i クライアント計算機 ($i = 0, 1, 2, \dots, n$)
 - 11 CPU
 - 12 メモリ
 - 13 不揮発メモリ
 - 14 入力部
 - 15 表示部
 - 17 アクセス制御表
 - 18 アクセス制御表管理部
 - 19 有効時間制御部
 - 20 クライアント識別情報取得部
 - AF(i) アクセス許可フラグ
 - T(i) 有効時間
 - CA(i) クライアントアドレス
- なお、各図中同一符号は同一または相当部分を示す。

【図3】



【図 1】



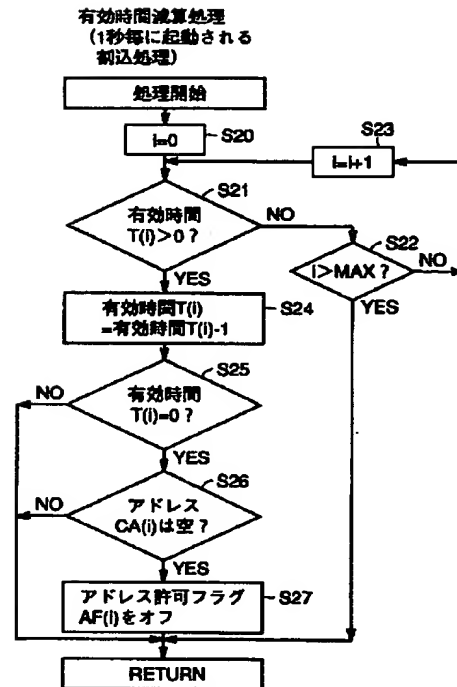
(B)

17

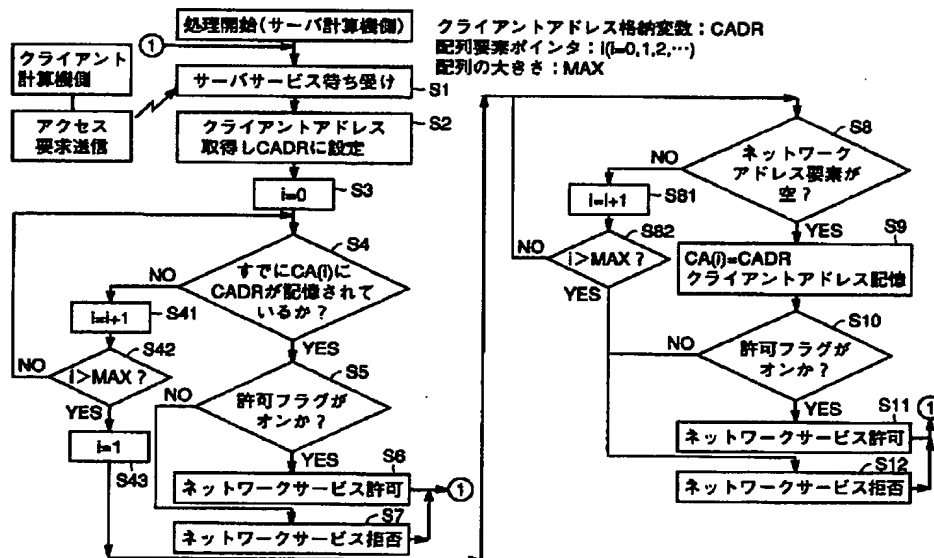
| i | AF(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|------------------|------------|-------------------|
| 0 | AF(0) | T(0) | CA(0) |
| 1 | AF(1) | T(1) | CA(1) |
| ⋮ | ⋮ | ⋮ | ⋮ |
| n | AF(n) | T(n) | CA(n) |

i=0,1,2,3,...,n

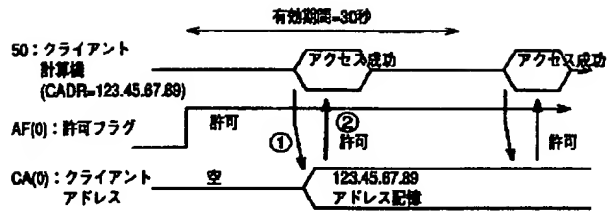
【図 5】



【図 4】



【図6】



【図8】

17

| | F(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|-----------------|------------|-------------------|
| 0 | オン | 30 | |
| 1 | オフ | 0 | |
| 2 | オフ | 0 | |

【図10】

17

| | F(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|-----------------|------------|-------------------|
| 0 | オン | 25 | 123.45.67.89 |
| 1 | オフ | 0 | 123.45.67.90 |
| 2 | オフ | 0 | |

【図12】

17

| | F(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|-----------------|------------|-------------------|
| 0 | オン | 25 | 123.45.67.89 |
| 1 | オン | 0 | 123.45.67.90 |
| 2 | オン | 30 | |

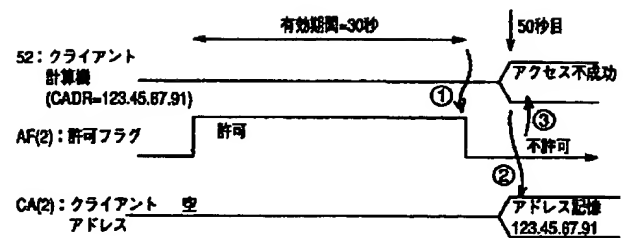
【図14】

15

サーバ管理テーブル

| | クライアントアドレス | |
|--|--------------|----------|
| <input checked="" type="checkbox"/> 許可 | 123.45.67.89 | アドレスリセット |
| <input type="checkbox"/> 許可 | | アドレスリセット |
| <input type="checkbox"/> 許可 | | アドレスリセット |

【図7】



【図9】

17

| | F(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|-----------------|------------|-------------------|
| 0 | オン | 25 | 123.45.67.89 |
| 1 | オフ | 0 | |
| 2 | オフ | 0 | |

【図11】

17

| | F(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|-----------------|------------|-------------------|
| 0 | オン | 25 | 123.45.67.89 |
| 1 | オン | 0 | 123.45.67.90 |
| 2 | オフ | 0 | |

【図13】

17

| | F(i): アクセス許可フラグ | T(i): 有効時間 | CA(i): クライアントアドレス |
|---|-----------------|------------|-------------------|
| 0 | オン | 25 | 123.45.67.89 |
| 1 | オン | 0 | 123.45.67.90 |
| 2 | オフ | 0 | 123.45.67.91 |

フロントページの続き

- (54) 【発明の名称】 通信ネットワークにおける簡易セキュリティ設定方法およびそのための装置、ならびに通信ネットワークにおける簡易セキュリティ設定プログラムを記録したコンピュータで読取可能な記録媒体